THE SHORTEST VECTOR PROBLEMS IN p-ADIC APPROXIMATION LATTICES AND THEIR APPLICATIONS TO CRYPTOGRAPHY (Nonlinear Analysis and Convex Analysis)

AUTHOR(S):

井上, 裕仁; 内藤, 幸一郎

CITATION:

井上, 裕仁 ...[et al]. THE SHORTEST VECTOR PROBLEMS IN p-ADIC APPROXIMATION LATTICES AND THEIR APPLICATIONS TO CRYPTOGRAPHY (Nonlinear Analysis and Convex Analysis). 数理解析研究所講究録 2015, 1963: 16-23: KJ00010016381.

ISSUE DATE:

2015-10

URL:

http://hdl.handle.net/2433/224191

数理解析研究所講究録
第1963巻 2015年 16-23

THE SHORTEST VECTOR PROBLEMS IN p-ADIC APPROXIMATION LATTICES AND THEIR APPLICATIONS TO CRYPTOGRAPHY

HIROHITO INOUE AND KOICHIRO NAITO

DEPARTMENT OF APPLIED MATHEMATICS, GRADUATE SCHOOL OF SCIENCE AND TECHNOLOGY, KUMAMOTO UNIVERSITY

1. Introduction

In this paper we combined the two problems; the shortest vector problems (SVP) in p-adic lattices and the simultaneous approximation problems (SAP) of p-adic numbers, by using the geometry of p-adic numbers as the glue. These two problems have the computational complexity, NP-hardness or NP-completeness. The security of the modern cryptosystems is based on the hardness of these problems and the lattice-based cryptography is considered as the most powerful post-quantum cryptography. In the usual real numbers case the inhomogeneous simultaneous approximations problems (ISAP), which are NP-complete, are used to construct cryptographic systems. Showing the relations between the shortest vectors in the p-adic approximation lattices and the integer solutions of p-adic SAP or ISAP, we propose a new cryptosystem given by using SAP or ISAP.

We construct multi-dimensional p-adic approximation lattices by simultaneous rational approximations of p-adic numbers. For analyzing these p-adic lattices we apply the LLL algorithm due to Lenstra, Lenstra and Lovász, which has been widely used to solve the various NP problems such as SVP (Shortest Vector Problems), ILP (Integer Linear Programing) .. and so on. Theoretically it is known that the LLL algorithm approximately solves SVP within a factor of $2^{O(n)}$ for the lattice dimension $n(\geq 3)$ in polynomial times. Using the LLL reduction algorithm in the open source software Sage, we numerically show that these SVP or SAP solutions of the lattice dimensions under 60 satisfy these exact estimates in the l_∞ norm.

In the second part, using these numerical results we propose a new lattice based cryptosystem where we choose a n-tuple of p-adic integers as public keys and we set the SAP solutions of these numbers as private keys. Since we can numerically show that the l_∞ norms of the SVP solutions given by LLL in the lattices of dimensions over 60 exceed the boundary value $p^{m/(n+1)}$ of the SAP solutions, the private keys given in the lattices of dimensions over this value are considered to be secure for the attacks by LLL.

2010 *Mathematics Subject Classification.* 11E95, 11A55, 14G50.
Key words and phrases. P-adic theory, LLL algorithm, Cryptography.

Our plan of this paper is as follows. In Section 2 we introduce the p-adic approximation lattices and we estimate the l_∞ norm of p-adic SAP solutions. In Section 3 we give the numerical estimates of the SAP solutions by using the LLL reduction algorithm. In Section 4 and 5 we propose new cryptosystems based on the results in the preceding sections.

2. p-ADIC LATTICE

In this section we introduce p-adic approximation lattices and investigate simultaneous rational approximations of p-adic numbers. Let p be a fixed rational prime number and $|\cdot|_p$ be the corresponding p-adic valuation, normalized so that $|p|_p = p^{-1}$. The completion of $\mathbb{Q}$ w.r.t. $|\cdot|_p$ is called the field of p-adic numbers, denoted by $\mathbb{Q}_p$. The strong triangle inequality

$$|a+b|_p \le \max\{|a|_p, |b|_p\}, \quad a, b \in \mathbb{Q}_p$$

is most important and essential to construct p-adic approximation lattices. The set of p-adic integers is defined by $\mathbb{Z}_p = \{z \in \mathbb{Q}_p : |z|_p \le 1\}$.

Let $n \ge 1$ be an integer and let $\Xi = \{\xi_1, \xi_2, \ldots, \xi_n\}$ be a n-tuple of p-adic integers.

Definition 2.1. We denote by $w_n(\Xi)$ the supremum of the real numbers w such that, for some infinitely many real numbers X_j, which goes to infinity, the inequalities

$$0 < |a_{0,j} + a_{1,j}\xi_1 + \cdots + a_{n,j}\xi_n|_p \le X_j^{-w-1},$$
$$\max_{0 \le i \le n} |a_{i,j}| \le X_j,$$

have a solution in integers $a_{0,j}, a_{1,j}, \ldots, a_{n,j}$.

For a positive integer m we define the p-adic approximation lattice Γ_m by

$$\Gamma_m = \{(a_0, a_1, \ldots, a_n) \in \mathbb{Z}^{n+1} : |a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \le p^{-m}\}. \tag{2.1}$$

When a p-adic integer ξ_i has the p-adic expansion

$$\xi_i = \sum_{k=0}^{\infty} x_{i,k} p^k, \ 0 \le x_{i,k} \le p-1,$$

let $\xi_{i,m}$ be the m-th order approximation of ξ_i defined by

$$\xi_{i,m} = \sum_{k=0}^{m-1} x_{i,k} p^k. \tag{2.2}$$

Consider the basis $\{b_{0,m}, b_{1,m}, \ldots, b_{n,m}\} \subset \mathbb{Z}^{n+1}$ of the lattice Γ_m given by

$$b_{0,m} = (p^m, 0, \ldots, 0)^t, \quad b_{1,m} = (\xi_{1,m}, -1, 0, \ldots, 0)^t,$$
$$b_{2,m} = (\xi_{2,m}, 0, -1, 0, \ldots, 0)^t, \cdots, b_{n,m} = (\xi_{n,m}, 0, \ldots, 0, -1)^t.$$

In fact, we have $b_{k,m} \in \Gamma_m$, $\forall k$, since we can estimate

$$|\xi_{k,m} - \xi_k|_p \le p^{-m}.$$

For $B_m = (b_{0,m} b_{1,m} \dots b_{n,m})$ we have

$$B_m = \begin{pmatrix} p^m & \xi_{1,m} & \xi_{2,m} & \cdots & \xi_{n,m} \\ 0 & -1 & 0 & \dots & 0 \\ 0 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & -1 \end{pmatrix}, \quad |\det(B_m)| = p^m.$$

Applying the LLL algorithm for $\delta \in (1/4, 1)$, we denote $\{b_0, b_1, \dots, b_n\}$ a reduced basis and $B = (b_0\ b_1\ \dots\ b_n)$. It is known that the shortest vector b_0 in B satisfies

$$\begin{aligned} \|b_0\|_2 &\le \sqrt{n+1}\ |\det(B)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\ &= \sqrt{n+1}\ |\det(B_m)|^{\frac{1}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n \\ &= \sqrt{n+1}\ p^{\frac{m}{n+1}} \left(\frac{2}{\sqrt{4\delta - 1}}\right)^n. \end{aligned} \tag{2.3}$$

Now we estimate the minimum norm value $\lambda_1^{(\infty)}(\Gamma_m) (= \lambda_1^{(\infty)}(B_m))$ by using the famous Dirichlet principle.

Theorem 2.2. *For a n-tuple of p-adic integers $\Xi = \{\xi_1, \dots, \xi_n\}$, which are irrational and linearly independent over $\mathbb{Q}$, and each positive integer m, there exists a solution in integers $a_{0,m}, a_{1,m}, \dots, a_{n,m} \in \mathbb{Z}^{n+1}$, which satisfies*

$$0 < |a_{0,m} + a_{1,m}\xi_1 + \cdots + a_{n,m}\xi_n|_p \le p^{-m}, \tag{2.4}$$

$$\max_{0 \le i \le n} |a_{i,m}| \le p^{\frac{m}{n+1}}. \tag{2.5}$$

Consequently, we have

$$\lambda_1^{(\infty)}(\Gamma_m) \le p^{\frac{m}{n+1}} = \det(\Gamma_m)^{\frac{1}{n+1}}. \tag{2.6}$$

3. Numerical calculations on SAP

In this section, we compare the minimum norms of the vectors given by the LLL reduction algorithm and the upper bound of the norms of the shortest vectors $X_m := p^{m/(n+1)}$ given in Theorem 2.2, using the open source software Sage. We investigate the following case.

$p = 13$: prime number,

$\xi_i = u_i^{\frac{1}{103}}$: p-adic number, 103rd root of u_i:

11, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29, 30, 31, 32,
33, 34, 35, 36, 37, 38, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 53, 54,
55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75,
76, 77, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 92, 93, 94, 95, 96, 97

$m = 5, 6, \dots, 40$: approximation orders

$n = 20, 60, 80$: dimensions

First we show our numerical process by using the small parameters, $n = 10$, $\xi_i = u_i^{\frac{1}{103}}$, $m = 5$. For the approximation order $m = 5$ and the dimension $n = 10$, we apply the LLL reduction ($\delta = 0.99999$). Then we obtain the reduced basis B from B_m. Here we note that the basis is given by row vectors in Sage.

$$B_m = \begin{pmatrix} 371293 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 125400 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 286272 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 282218 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 340728 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 128378 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 4671 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 341596 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 366035 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 6311 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 348639 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

$$B = \begin{pmatrix} 0 & -1 & -1 & -1 & -1 & 2 & 0 & 0 & 0 & 2 & -1 \\ 0 & 1 & 2 & -1 & 1 & 0 & -2 & -1 & 1 & -1 & 1 \\ 1 & 1 & -2 & 2 & 0 & -1 & 0 & 0 & 1 & -1 & -1 \\ 0 & -1 & 2 & 2 & 0 & 1 & 1 & 1 & -1 & -1 & 0 \\ 2 & -1 & 1 & 0 & -2 & 1 & 2 & 0 & -1 & 1 & 0 \\ -1 & 0 & 1 & 0 & -1 & 0 & 0 & -1 & 2 & 2 & -1 \\ 0 & -1 & -2 & 0 & 2 & 0 & 1 & -1 & 1 & -2 & 0 \\ -1 & 1 & -1 & -1 & 0 & 0 & -1 & -3 & 0 & -2 & 0 \\ 0 & 0 & 0 & -1 & 1 & -1 & -2 & -1 & -2 & -1 & -2 \\ 1 & -2 & -1 & 2 & -1 & 0 & 0 & 0 & 0 & -2 & 2 \\ 1 & -1 & 0 & 1 & 1 & -1 & -1 & 0 & -2 & 3 & 1 \end{pmatrix}.$$

We obtain

$$\min_{0\le i\le n} \|b_i\|_2 = 3.60555..., \quad \max_{0\le i\le n} \|b_i\|_2 = 4.35889...,$$
$$\min_{0\le i\le n} \|b_i\|_\infty = 2, \quad \max_{0\le i\le n} \|b_i\|_\infty = 3,$$

which are sufficiently effective solutions of SVP, smaller than the value $X_m = p^{m/(n+1)} = 3.208764...$, comparing the theoretical estimate (2.6) in Theorem 2.2

$$\lambda_1^{(\infty)}(\Gamma_m) \le p^{\frac{m}{n+1}} = \det(\Gamma_m)^{\frac{1}{n+1}}.$$

Next we give the graphs which compare these numerical minimum and maximum values in the l_∞ norm and the minimum values in the l_2 norm for the shortest vectors given by the LLL reduction basis and the values X_m for the approximation orders m from 5 to 40 and the dimensions $n = 20, 60, 80$.

Since the LLL reduction algorithm approximately finds the shortest vectors in the l_2 norm, we use their l_∞ norm values as the substitutes of the shortest vectors in the l_∞ norm. We use the following line styles in the graphs.

— · — · — · — : minimum norm values of the reduced basis vectors in l_2

- - - - - - - - : maximum norm values of the reduced basis vectors in l_∞

———— : $X_m = p^{m/(n+1)}$

· · · · · · · · · · · · : minimum norm values of the reduced basis vectors in l_∞

These graphs show that the LLL algorithm is effective enough to obtain the solutions of SAP, which satisfy the estimate (2.6), if the dimension n is under 60 (see Figure 1 and 2), but this estimate is not satisfied for some m if $n > 60$ and if $n \geq 80$ and $m \geq 30$.

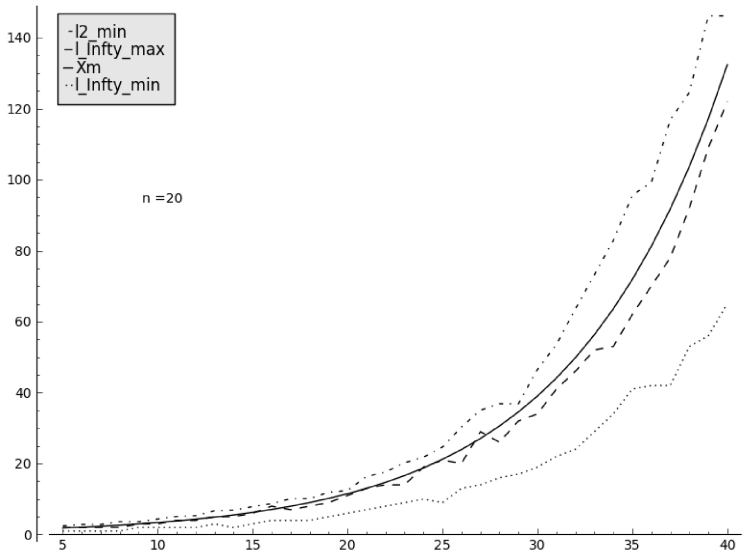

FIGURE 1. $n = 20$

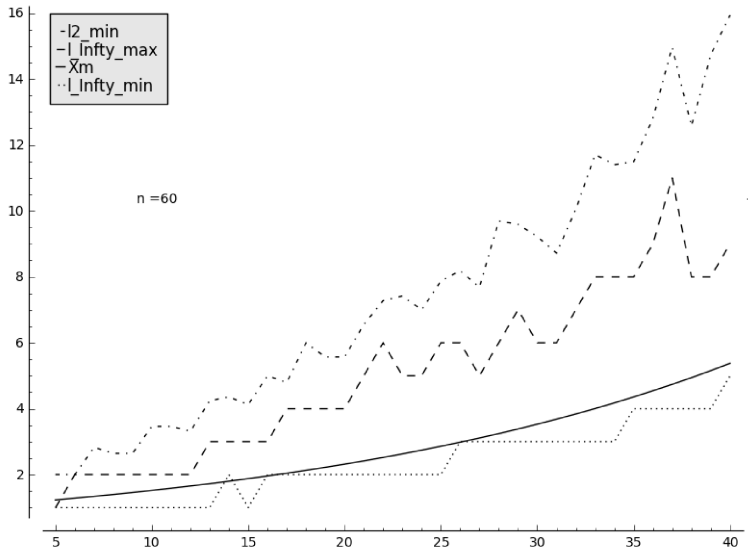

FIGURE 2. $n = 60$

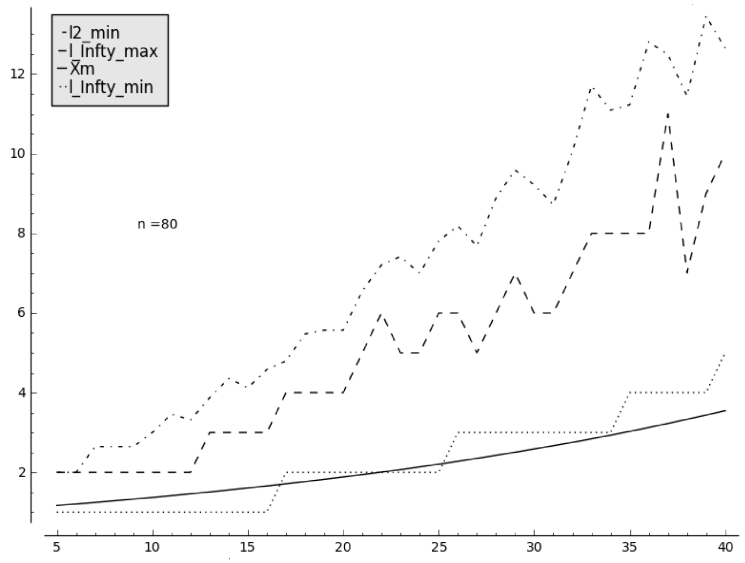

FIGURE 3. $n = 80$

4. CRYPTOSYSTEM I

In this section we propose a new cryptosystem, the security of which depends on the hardness of solving the SAP. Now we assume that Alice wants to send a message to Bob in this cryptosystem.

Key generation

First, we choose a prime number p and $m \in \mathbb{N}$, which are the common private keys of Alice and Bob.. For a public key we set a l-tuple of p-adic integers $\{\eta_1, \ldots, \eta_l\}$, which satisfies

$$|\eta_1|_p > |\eta_2|_p > \cdots > |\eta_l|_p, \ \eta := (\eta_1, \ldots, \eta_l), \tag{4.1}$$

and we construct a n-tuple of irrational p-adic integers $\{\xi_1, \ldots, \xi_n\}$ as a public key, linearly independent over $\mathbb{Q}$, and a $n+1$-tuple of rational integers $\{a_0, a_1, \ldots, a_n\}$ as a secret key, which satisfies $|a_i| \leq p^{m/(n+1)}, i = 0, \ldots, n$ and $|a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \leq p^{-m}$ as follows.

We randomly choose the integers $a_0, \ldots, a_{n-1}$ which satisfy the condition $|a_i| \leq p^{m/(n+1)}, i = 0, \ldots, n-1$, and put $a_n = 1$. Next we randomly choose a linearly independent n-tuple of p-adic integers $\{\xi_0, \xi_1, \ldots, \xi_{n-1}\}$, satisfying $|\xi_0|_p \leq p^{-m}$, and we define ξ_n by $\xi_n = \xi_0 - (a_0 + a_1\xi_1 + \cdots + a_{n-1}\xi_{n-1})$. Then we have $|\xi_n + (a_0 + a_1\xi_1 + \cdots + a_{n-1}\xi_{n-1})|_p \leq p^{-m}$. Thus the set of these integers $\{a_0, \ldots, a_n\}$ becomes a solution of SAP :

$$0 < |a_0 + a_1\xi_1 + \cdots + a_n\xi_n|_p \leq p^{-m}, \tag{4.2}$$

$$\max_{0 \leq i \leq n} |a_i| \leq p^{\frac{m}{n+1}}. \tag{4.3}$$

The security of the secret key $\{a_0, \ldots, a_n\}$ depends on the NP-hardness of the SAP.

Encryption

For a plaintext $\mathbf{x} = (x_1, \ldots, x_l) \in \{0,1\}^l$, Alice constructs its linear combination as a part of ciphertext $\mathbf{c}_0$ by

$$\mathbf{c}_0 := \mathbf{x} \cdot \eta = \sum_{i=1}^{l} x_i \eta_i.$$

By using $\eta = (\eta_1, \ldots, \eta_l)$, which satisfies (4.1), instead of the superincreasing sequence in the Knapsack cryptosystem Bob can easily decrypt the ciphertext $\mathbf{c}_0$ into the plaintext $\mathbf{x}$.

Alice constructs her ciphertext $\mathbf{c}$ by

$$\mathbf{c} = p^{-m}(a_0 + a_1\xi_1 + \cdots + a_n\xi_n) + \mathbf{c}_0$$

and she sends $\mathbf{c}$ to Bob.

Decryption

Bob obtains the part of the ciphertext $\mathbf{c}_0$ by using the public keys and the secret key from the ciphertext $\mathbf{c}$.

$$\mathbf{c} - p^{-m}(a_0 + a_1\xi_1 + \cdots + a_n\xi_n) = \mathbf{c}_0 = \mathbf{x} \cdot \eta.$$

The plaintext $\mathbf{x}$ is recovered from $\mathbf{c}_0$ step by steps as follows.

1st-step: If $|\mathbf{c}_0|_p \geq |\eta_1|_p$, then $x_1 = 1$, otherwise $x_1 = 0$.

2nd-step: If $|\mathbf{c}_0 - x_1\eta_1|_p \geq |\eta_2|_p$, then $x_2 = 1$, otherwise $x_2 = 0$.

$\vdots$

lth-step: If $|\mathbf{c}_0 - (x_1\eta_1 + \cdots + x_{l-1}\eta_{l-1})|_p \geq |\eta_l|_p$, then $x_l = 1$, otherwise $x_l = 0$.

5. Cryptosystem II (practical variations)

In this section we give some practical variations of Cryptosystem I to increase its security. Instead of the public keys of p-adic integers $\eta_1, \ldots, \eta_l$, p-adic absolute values of which are decreasing, let $\eta_1, \ldots, \eta_l$, be units and consider the two common secret keys, a permutation $\varphi(i) : \{1, \ldots, l\} \to \{1, \ldots, l\}$ and a strictly increasing sequence of positive integers $\{m_i\}_{1 \leq i \leq l}$: $m_1 < m_2 < \cdots < m_l < m$.

Let the secret key a_i be the sum of α_i and β_i, that is

$$a_i = \alpha_i + \beta_i, \ \alpha_i, \beta_i \in \mathbb{Z}, \ i = 0, 1, \ldots, n.$$

Alice has the secret key $\{\alpha_i\}$ and Bob has the secret key $\{\beta_i\}$.

Encryption

Alice constructs the part of the ciphertext $\mathbf{c}_0$ by

$$\mathbf{c}_0 = \sum_{i=1}^{l} x_i p^{m_{\varphi(i)}} \eta_{\varphi(i)}.$$

and she constructs the ciphertext $\mathbf{c}_A$ by

$$\mathbf{c}_A = \alpha_0 + \alpha_1\xi_1 + \cdots + \alpha_n\xi_n + \mathbf{c}_0.$$

Decryption

Bob takes the sum of $\mathbf{c}_A$ and the linear combination of $\{\xi_1, \ldots, \xi_n\}$ with his secret key. Then he has

$$\mathbf{c}_A + \beta_0 + \beta_1\xi_1 + \cdots + \beta_n\xi_n \;=\; a_0 + \sum_{j=1}^{n} a_j\xi_j + \sum_{i=1}^{l} x_{\varphi^{-1}(i)}p^{m_i}\eta_i := \mathbf{c}_B.$$

Since $(a_0, \ldots, a_n)$ is an integer solution of the SAP and $m > m_l > \cdots > m_1$, it follows from the isosceles principle that

$$|\mathbf{c}_B|_p = |a_0 + \sum_{j=1}^{n} a_j\xi_j + \sum_{i=1}^{l} x_{\varphi^{-1}(i)}p^{m_i}\eta_i|_p = |\sum_{i=1}^{l} x_{\varphi^{-1}(i)}p^{m_i}\eta_i|_p$$

if $\mathbf{x} \neq (0, 0, \ldots, 0)$.

The plaintext $\mathbf{x}$ is recovered from $\mathbf{c}_B$ step by steps and Bob can easily recover the message $\mathbf{x}$ from $\mathbf{c}_0$ by using the secret keys $\varphi(i), \{m_i\}$ and the Knapsack type procedure.

References

1. Y.Bugeaud, "Approximation by Algebraic Numbers", Cambridge Tracts in Mathematics, Cambridge University Press, 2004.
2. J.W.S.Cassels, "An introduction to Diophantine approximation", Cambridge Tract 45, Cambridge Univ. Press, 1957
3. Y.A.Khinchin, "Continued Fractions", the University of Chicago Press 1964. 28 # 5037
4. D. Micciancio and S. Goldwasser, "Complexity of Lattice Problems, a Cryptographic Perspective", Springer International Series in Engineering and Computer Science, vol. 671. Springer, 2002
5. P.Q. Nguyen and B. Vallee (Eds.), "The LLL Algorithm, Survey and Applications", Springer 2010.
6. W.M.Schmidt, "Diophantine Approximation", Springer Lecture Notes in Math. 785, 1980.
7. V.G. Sprindžuk, Mahler's problem in metric number theory. Izdat. "Nauka i Tehnika", Minsk, 1967 (in Russian). English translation by B. Volkmann, Translations of Mathematical Monographs, Vol. 25, American Mathematical Society, Providence, R.I., 1969

Department of Applied Mathematics,
Graduate School of Science and Technology,
Kumamoto University,
Kurokami 2-39-1, Kumamoto, Japan
132d9307@st.kumamoto-u.ac.jp
knaito@gpo.kumamoto-u.ac.jp

熊本大学大学院・自然科学研究科　井上 裕仁
熊本大学大学院・自然科学研究科　内藤 幸一郎